UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,882	10/28/2003	Jae Deok Lim	P69238US0	4036

136 7590 11/06/2006

JACOBSON HOLMAN PLLC
400 SEVENTH STREET N.W.
SUITE 600
WASHINGTON, DC 20004

EXAMINER	
KOEMPEL THOMAS, BEATRICE L	

ART UNIT	PAPER NUMBER
2196	

DATE MAILED: 11/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/693,882	LIM ET AL.	
	Examiner	Art Unit	
	Bea Koempel-Thomas	2196	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-9 are pending in this application and presented for examination.

Objections

Specification

2. The specification is replete with terms that are not clear, concise and exact. The specification should be revised carefully in order to avoid the introduction of new matter.

Examples of some unclear, inexact or verbose terms used in the specification are: page 4 line 3, "such as MAC," and page 4 line 14, "security class and category of the MAC." Mandatory Access Control (MAC) is being construed as a "policy specifi[ng] how subjects may access objects under the control of the operating system." Loscocco, Peter A. et al, "The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments," National Security Agency, 1998, page 2. This would be known to one of ordinary skill in the art and consistent with the disclosure of the specification. Examiner believes security class and category reasonably include any type of class used for security and any category, and so interpreted security class or category in this case.

Additional examples: page 7 line 3; "next protocol field," page 9 line 24 " a next protocol area." Using both "area" and "field" represents inexact terminology as applicant apparently intended to represent the same element. Similar inexact terminology is repeated on additional elements in the claims.

Additional examples: page 10 lines 1-2, "a MAC class and a MAC category," line 12 "a MAC security class," page 11 line 3 "the MAC class and category," page 14 lines 9, 15, and 24

"a security class," page 15, line 4 "security information (class and category)." Such multiple permutations of MAC, security, class, category, and information cause the specification to be unclear and inexact.

Further examples: page 4 line 21, "there is provided an apparatus for providing," "there is provided a method for providing." Page 9 line 18, "In case a trusted channel is applied to the packet." Redundant circuitous terminology is unacceptably verbose and causes lack of clarity in the application. Applicant is advised to correct all similar awkward and verbose language repeated throughout the specification.

3. The specification is objected to for the following informality: page 17 line 10 the term "deserted" was apparently substituted for "discarded" as suggested by Figure 2A, step 217.

4. A substitute specification in proper idiomatic English and in compliance with 37 CFR 1.52(a) and (b) is required. The substitute specification filed must be accompanied by a statement that it contains no new matter.

5. The substitute specification must be submitted with markings showing all the changes relative to the immediate prior version of the specification of record. The text of any added matter must be shown by underlining the added text. The text of any deleted matter must be shown by strikethrough except that double brackets placed before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted matter must be shown by being placed within double brackets if strikethrough cannot be easily perceived. An accompanying clean version (without markings) and a statement that the substitute specification contains no new matter must also be supplied. Numbering the paragraphs of the specification of record is not considered a change that must be shown.

Claim Objections

6. Claims 2-9 are objected to because of the following informalities: non-idiomatic English. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors. Examples follow.

Claim 2: "[A]pplication of the trusted channel is determined in case of data transmission, if two requirements are satisfied: a destination address of the packet should correspond to one of the host addresses to which the trusted channel is applied and the user should have a MAC security class and if the application of the trusted channel is determined, the application of the trusted channel is indicated." To further prosecution, the examiner considered the claim as though the quoted section read: "for data transmission, a trusted channel should be applied when both of the following requirements are satisfied: a destination address of the packet corresponds to one of the host addresses to which the trusted channel should be applied and the user has a MAC security class."

Claim 3: "application of the trusted channel is investigated, in case of data reception, by checking whether the next protocol field of the IP header of the packet represents the trusted channel header." To further prosecution, the examiner considered the claim as though the quoted section read: "upon data reception, check if the next protocol field of the IP header of the packet represents the trusted channel header."

Claim 4: "a MAC class and a MAC category area." To further prosecution, the examiner considered the claim as though the quoted section read: "a MAC class **area** and a MAC category area."

Claim 5: "wherein encryption area." To further prosecution, the examiner considered the claim as though the quoted section read: "wherein **an** encryption area."

Claim 6: "(b) creating a trusted channel header for storing therein information generated at a time when the trusted channel is applied and security information, i.e., a class and a category, of the user if the application of the trusted channel is determined in the step (a); (c) . . . an authentication data portion and an initial vector portion; generating authentication information for an integrity of the packet; and storing the authentication information in the trusted channel header." To further prosecution, the examiner considered the claim as though the quoted section read: "creating a trusted channel header for storing therein information generated when the trusted channel is applied and security information, **that is,** a **MAC** class and a **MAC** category, of the user if the application of the trusted channel is determined in the step (a); (c) . . . an authentication data **field** and an initial vector **field**; generating authentication information for **validating** the packet; and storing the authentication information in the trusted channel header;"

Applicant is advised to correct all similar unclear, indefinite, and awkward language and syntax repeated throughout the application.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,076,168 to William Alton Fiveash et al (hereinafter "Fiveash") in view of U.S. Patent 5,937,159 to William J. Meyers et al (hereinafter "Meyers").

9. Regarding **claim 1**, Fiveash discloses an apparatus for providing a trusted channel among operating systems to which a mandatory access control (MAC) policy is applied (column 2 lines 50-51 internet protocol security system), the apparatus comprising:

on a data transmission side:

a kernel memory (column 5 line 45 "kernel")

for specifying host addresses to which the trusted channel is to be applied (column 5 lines 43-47 "reading the description of the tunnel . . . and insert[ing] it into a kernel for use by IP traffic," the description includes the destination address) and

providing an encryption key for encryption of a packet (column 5 line 47 "encryption algorithm") and

an authentication key for generation of authentication data (column 5 lines 46-47 "authentication algorithm"); and

a trusted channel sub system (Figure 1 and column 2 lines 51-53 "an IP stack 110, a filter module 120, a tunnel module 130")

for determining whether or not to apply the trusted channel, if data to be transmitted to IP layer is provided from the user, by using the host addresses to which a trusted channel is to be applied from the kernel memory (column 2 lines 58-60 "Filter module 120 and tunnel module 130 contain all the filter rules and tunnel definitions, respectively, used by the host system");

creating a trusted channel header if the application of the trusted channel is determined (column 3 lines 15-18 "If the data is to be encrypted and should be authenticated by the remote host, it is encrypted and the headers ESP and AH added before it is passed to the network");

encrypting a specific portion of the packet (column 1 lines 50-56 "When defining a tunnel, a user can choose to encapsulate the entire data packet including IP headers or just the data itself. . . . Encapsulation of only the data is ordinarily done when a trusted network is used.");

storing the authentication data in the trusted channel header (column 3 lines 15-18 "If the data is to be encrypted and should be authenticated by the remote host, it is encrypted and the headers ESP and AH added before it is passed to the network); and

transmitting the packet through a network (column 3 lines 17-18 "it [the packet] is passed to the network");

on a data reception side:

a trusted channel sub system (column 2 lines 51-53 "an IP stack 110, a filter module 120, a tunnel module 130")

for investigating whether the trusted channel is applied (column 2 lines 63-66 "it is determined whether the data packet is encrypted and/or whether authentication is required. If so, the data packet is decrypted and/or authenticated");

retrieving the authentication data in the trusted channel header (column 2 lines 65-66 "If [authentication is required], the data packet is . . . authenticated");

decrypting the packet if the authentication data is valid (column 2 lines 63-67 and column 3 line 1 "If [the data packet is encrypted and/or authentication is required] the data packet is decrypted and/or authenticated . . . Then it is determined whether authentication or decryption of the packet has failed . . . If yes, the packet is dropped");

conducting trusted channel header processings (column 3 lines 35-37 "Rules 2 and 3 are used to allow processing of AH and ESP headers, respectively"); and

transferring the packet to an upper level by following a routine for delivering the packet to an input processing section of the upper level to thereby provide the packet to a user on the data reception side (column 3 lines 5-6 "the data packet is passed to the application layer"); and

a kernel memory for providing an authentication key for the authentication of the packet and an encryption key for the decryption of the packet (column 5 line 45 "kernel").

Fiveash does not explicitly disclose secure operating systems (OSs), or a MAC module for providing MAC information of a user on a data transmission side.

Meyers teaches a secure operating system (OS) (column 2 line 65). Meyers further teaches a MAC module for providing MAC information of a user on a data transmission side (column 6 lines 9-10 "MAC . . . controls a subject's access to information and objects").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of configuring internet protocol security tunnels disclosed in Fiveash for use with the secure operating systems and MAC information taught by Meyers to automate the creation of a tunnel between secure operating systems based on user status.

10. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fiveash and Meyers further in view of U.S. Patent 5,983,350 to Spence Minear et al (hereinafter "Minear").

11. Regarding **claim 2**, Fiveash discloses application of the trusted channel being determined upon data transmission, if two requirements are satisfied: (column 5 lines 26-27 "A minimum set of parameters are necessary to identify a tunnel"). Meyers discloses that the user should have a MAC security class (column 6 lines 21-25 "The label consists of a hierarchical component

(classification of information sensitivity) and one or more categories (unrelated groups of users) following the syntax: hierarchy: (category1, category2 . . .)").

Fiveash and Meyers do not disclose the packet's destination address corresponding to one of the host addresses to which the trusted channel is applied. Minear teaches a destination address of the packet corresponding to one of the host addresses to which the trusted channel is applied (column 4 lines 31-33 "the sending firewall uses the . . . Destination Address to select an appropriate Security Association").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the minimum parameters of Fiveash and MAC labels of Meyers with Minear's use of destination address to determine when a secure communication mode is necessary.

12. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fiveash, Meyers and Minear further in view of S. Kent, BBN Corp., "Security Architecture for the Internet Protocol, Request for Comments: 2401", November 1998, (hereinafter "RFC 2401").

13. Regarding **claim 3**, Fiveash, Meyers and Minear do not disclose application of the trusted channel being investigated, in case of data reception, by checking whether the next protocol field of the IP header of the packet represents the trusted channel header.

However, RFC 2401 discloses application of the trusted channel being investigated, in case of data reception, by checking whether the next protocol field of the IP header of the packet represents the trusted channel header (page 33 paragraph 4 "Each inbound IP datagram to which

IPsec processing will be applied is identified by the appearance of the AH or ESP values in the IP Next Protocol field").

Therefore, it would have been obvious to one skilled in the art at the time of the invention to combine the use of the next protocol field as taught by RFC 2401 with the teachings of the internet security protocol of Fiveash, Meyers and Minear in order to expedite proper packet processing.

14. Claims 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fiveash, and Meyers in view of RFC 2401, and further in view of S. Kent, BBN Corp., "IP Encapsulating Security Payload (ESP), Request for Comments: 2406", November 1998, (hereinafter "RFC 2406").

15. Regarding **claim 4**, Fiveash discloses the trusted channel header including an authentication data area for guaranteeing an integrity of the encrypted data (column 1 line 43 "authentication header"), and an initial vector area for the decryption of the encrypted data (column 1 lines 46-48 "The receiving host is able to decrypt the data with a key shared with the transmitting host. Data that has been encrypted is referenced with an encryption header"). Meyers discloses a MAC class and a MAC category for delivering the MAC information of the user (column 6 lines 20-25 "MAC label—a label placed on subjects . . . in order to enforce the MAC policy. The label consists of a hierarchical component (classification of information sensitivity) and one or more categories (unrelated groups of users) following the syntax: hierarchy: (category1, category2 . . .)").

Fiveash and Meyers fail to disclose a next protocol area for a correct upper protocol processing, a header length area for identifying a length of the header, and a padding length area for indicating a length of padding used for data encryption.

RFC 2401 discloses a next protocol area for a correct upper protocol processing (page 18 paragraph 3 "IPv4 "Protocol" or the IPv6 "Next Header" fields"), and a header length area for identifying a length of the header, (page 31 paragraph 10 "header length")

RFC 2406 discloses a padding length area for indicating a length of padding used for data encryption (RFC 2406 page 7 paragraphs 2-3 "pad length").

As RFCs 2401 and 2406 are related documents, one skilled in the art at the time of the invention would have been motivated to refer to both of them to determine the standards for the state of the art in order to insure interoperability for security systems. Furthermore, it would have been obvious to one skilled in the art at the time of the invention to combine teachings of Fiveash, Meyers, RFC 2401, and the teachings of RFC 2406 to insure interoperability for security systems.

16. Regarding **claim 5**, Fiveash discloses an encryption area of the packet for maintaining security of the packet is set to be all areas thereof excluding an IP header area, the authentication data area and the initial vector area, (column 1 lines 50-56 "When defining a tunnel, a user can choose to encapsulate the entire data packet including IP headers or just the data itself. . . . Encapsulation of only the data is ordinarily done when a trusted network is used").

17. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fiveash in view of Meyers and further in view of RFC 2401.

18. Regarding **claim 6**, Fiveash discloses a method for providing a trusted channel among operating systems (OSs) (column 2 lines 50-51 internet protocol security system), including

a trusted channel sub system (Figure 1 and column 2 lines 51-53 "an IP stack 110, a filter module 120, a tunnel module 130"), a kernel memory on each of a data transmission side (column 5 lines 45 "kernel") and a data reception side (column 5 lines 30-32 "Both generated keys and specified keys are saved in the tunnel database") and

the method comprising the steps of:

(a) executing a packet output routine of an Internet Protocol (IP) layer if data to be transmitted to the IP layer is provided from the user (column 2 lines 58-60 "Filter module 120 and tunnel module 130 contain all the filter rules and tunnel definitions, respectively, used by the host system"); and searching the kernel memory on the data transmission side to determine whether or not to apply a trusted channel to a corresponding packet (column 5 lines 43-47 "tunnel database . . . reading the description of the tunnel . . . and insert[ing] it into a kernel for use by IP traffic," the description includes the destination address).

(b) creating a trusted channel header for storing therein information generated at a time when the trusted channel is applied and security information, i.e., a class and a category, of the user if the application of the trusted channel is determined in the step (a) (column 3 lines 15-18 "If the data is to be encrypted and should be

authenticated by the remote host, it is encrypted and the headers ESP and AH added before it is passed to the network");

(c) encrypting all areas of the trusted channel header excluding an authentication data portion and an initial vector portion (column 1 lines 50-56 "When defining a tunnel, a user can choose to encapsulate the entire data packet including IP headers or just the data itself. . . . Encapsulation of only the data is ordinarily done when a trusted network is used");

generating authentication information for an integrity of the packet (column 3 lines 15-18 "If the data is to be encrypted and should be authenticated by the remote host, it is encrypted and the headers ESP and AH added before it is passed to the network"); and

storing the authentication information in the trusted channel header (column 3 lines 15-18 "If the data is to be encrypted and should be authenticated by the remote host, it is encrypted and the headers ESP and AH added before it is passed to the network");

(d) conducting a checksum processing (column 1 lines 40-41 "checksum function") and a fragmentation processing (column 3 line 31 "Fragment_control") for the IP packet and providing the packet to the trusted channel sub system on the data reception side through a network by following a lower level output routine (Figures 1 and 3 column 3 lines 10-11 and 17-18 "data packet is moved to the IP stack . . . it is passed to the network");

(e) performing a reassembling processing (column 3 line 31 "Fragment_control") and a checksum processing (column 1 lines 40-41 "checksum function"), at a reception side IP input processing unit (column 3 lines 65-67 "defining the tunnel including associated filter rules on one end, creating a matching definition on the other end and activating the tunnel and filter rules on both ends"), for the packet received at the trusted channel sub system on the data reception side through the network and

(f) retrieving the authentication data in the trusted channel header before decrypting the packet if it is found in the step (e) that the trusted channel is applied to the packet (column 2 lines 63-66 "it is determined whether the data packet is encrypted and/or whether authentication is required. If so, the data packet is decrypted and/or authenticated"); and

decrypting the packet if the authentication data is valid while discarding the packet if the authentication data is not valid (column 2 lines 63-67 and column 3 line 1 "If [the data packet is encrypted and/or authentication is required] the data packet is decrypted and/or authenticated . . . Then it is determined whether authentication or decryption of the packet has failed . . . If yes, the packet is dropped"); and

(g) transferring the decrypted packet to an upper level by following a routine for delivering the packet to an input processing section of an upper level to thereby provide the packet to a user on the data reception side (column 3 lines 5-6 "the data packet is passed to the application layer").

Fiveash does not explicitly disclose secure operating systems (OSs), or searching a MAC module.

Meyers teaches a secure operating system (OS) (column 2 line 65). Meyers further teaches a MAC module for providing MAC information of a user on a data transmission side (column 6 lines 9-10 "MAC . . . controls a subject's access to information and objects").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of configuring internet protocol security tunnels disclosed in Fiveash for use with the secure operating systems and MAC information taught by Meyers to automate the creation of a tunnel between secure operating systems based on user status.

Fiveash and Meyers do not explicitly disclose investigating whether the trusted channel is applied to the packet by examining a next protocol field of an IP header in order to decrypt the packet. However, to do so is taught by RFC 2401 (page 33 paragraph 4 "Each inbound IP datagram to which IPsec processing will be applied is identified by the appearance of the AH or ESP values in the IP Next Protocol field").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine use of the next protocol field taught by RFC 2401 with the automatic configuration of internet security protocols taught by Fiveash and Meyers in order to accommodate full header processing.

19. Regarding **claim 7**, Fiveash discloses application of the trusted channel being determined by examining whether a destination address of the packet corresponds to one of the host addresses to which the trusted channel is applied (column 3 lines 26-27 "Destination_address").

Fiveash does not explicitly disclose the user having a MAC security class.

Meyers teaches a MAC security class (column 6 line 20 "MAC label").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of configuring internet protocol security tunnels disclosed in Fiveash for use with the MAC information taught by Meyers to automate the creation of a tunnel between secure operating systems based on user status.

20. Regarding **claim 8**, Fiveash does not disclose the trusted channel header being recorded in the next protocol field of an IP header of the packet to inform the user on the data reception side of the fact that the trusted channel is applied to the packet.

RFC 2401 teaches the trusted channel header being recorded in the next protocol field of an IP header of the packet to inform the user on the data reception side of the fact that the trusted channel is applied to the packet (page 33 paragraph 4 "Each inbound IP datagram to which IPsec processing will be applied is identified by the appearance of the AH or ESP values in the IP Next Protocol field").

Therefore, it would have been obvious to one skilled in the art at the time of the invention to combine the use of the next protocol field as taught by RFC 2401 with the internet security protocol of Fiveash and Meyers in order to assist the receiving user in identifying that a particular packet has had the security policy applied so that proper processing can occur expeditiously.

21. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fiveash in view of Meyers, and RFC 2401, and further in view of RFC 2406.

22. Regarding **claim 9**, Fiveash, Meyers, and RFC 2401 do not disclose a trusted channel header including a 128-bit authentication data field containing the authentication information for the encrypted packet, a 64-bit initial vector field used as encryption synchronization data of an encryption algorithm, a 8-bit next header field identifying an upper level protocol of IP, a 4-bit trusted channel header length field indicating a length in bytes of the trusted channel header, a 4-bit padding length field designating a length in bytes of a padding used for the encryption of the packet, and a 16-bit MAC class field and a 64-bit MAC category field showing MAC information of the user who requests the communication.

However, RFC 2406 teaches a secure packet format including an authentication field of variable length (page 7 paragraph 7), including an initialization vector in a variable-length payload field for encryption synchronization (page 5 paragraph 3), an 8-bit next header field identifying an upper layer protocol (page 7 paragraph 5), and an 8-bit pad length field indicating the number of pad bytes (page 7 paragraph 3).

Although RFC 2406 does not disclose a 4-bit trusted channel header length field, the pad length field being 4-bits, or a 16-bit MAC class field and a 64-bit MAC category field, it would be obvious to one skilled in the art at the time of the invention to use 4 bits of the 8-bit pad length field as a trusted channel header length field because the pad length and next header fields are to be right aligned in a 4-byte word so that the authentication field is aligned on a 4-byte boundary (page 6 paragraph 1). Doing so would facilitate the receiver efficiently processing the packet.

Therefore, it would have been obvious to one skilled in the art at the time of the invention to split the pad length field between trusted channel header length and pad length fields to achieve more efficient packet processing.

The authentication field of RFC 2406 includes an integrity check value of varying length requiring specification of the comparison rules and processing steps for validation (page 7 paragraph 7). Additionally, one skilled in the art at the time of the invention would have known that packet headers may have additional fields added and segmented as desired.

Therefore, it would have been obvious to one skilled in the art at the time of the invention to specify the MAC class field and MAC category fields as part of the integrity check to validate that the user appearing to request the communication was indeed the sending user.

Conclusion

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is:

- Department of Defense Standard, Department of Defense Trusted Computer System Evaluation Criteria, December 1985, DoD 5200.28-STD, regarding mandatory access control and incorporated classes and categories.
- Flyntz, Terence, U.S. Patent Publication US 2004/0015701 A1, regarding a multi-level and multi-category data labeling system.
- Loscocco, Peter A. et al, "The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments," National Security Agency, 1998, regarding mandatory access control.

Please direct any inquiry concerning this communication or earlier communications from the examiner to Bea Koempel-Thomas whose telephone number is 571-270-1252. The examiner can normally be reached on Monday - Thursday & alternate Fridays; 0730 - 1700.

If attempts to reach the examiner by telephone are unsuccessful, please contact the examiner's supervisor, Nabil El-Hady, on 571-272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

bkt 10/30/2006

NABIL M. EL-HADY
SUPERVISORY PATENT EXAMINER